In the Claims:

Claims 1-11 (Cancelled).

12. (New) A method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function, the method comprising:

decoding an input byte and generating at least one bit string that contains only one active bit;

logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string; and

encoding the 256-bit string for obtaining an output byte.

13. (New) A method according to Claim 12, wherein the decoding comprises subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the 256-bit string.

14. (New) A method according to Claim 12, wherein the input byte is decoded in a corresponding auxiliary 256-bit string; and the 256-bit string is obtained by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function.

15. (New) A method according to Claim 12, wherein the one-to-one binary function represents a ByteSub operation of a

2

Rijndael AES encryption/decryption algorithm.

16.   (New) A method according to Claim 13, wherein each bit of the 256-bit string is obtained by ANDing among the bits of the 16-bit strings.

17.   (New) A method for implementing a cryptographic algorithm comprising:

decoding an input byte and generating at least one bit string that contains at least one active bit;

logically combining bits of the at least one bit string according to the one-to-one binary function and generating a bit string; and

encoding the bit string for obtaining an output byte.

18.   (New) A method according to Claim 17, wherein the cryptographic algorithm comprises a Rijndael AES encryption/ decryption algorithm.

19.   (New) A method according to Claim 18, wherein the one-to-one binary function represents a ByteSub operation in the Rijndael AES encryption/decryption algorithm.

20.   (New) A method according to Claim 17, wherein the decoding comprises subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit; and wherein logically combining the bits comprises logically combining the 16-bit strings according to the one-to-one binary function for generating the bit string.

3

21.   (New) A method according to Claim 17, wherein the
input byte is decoded in a corresponding auxiliary bit string;
and the bit string is obtained by changing an order of the bits
of the auxiliary bit string according to the one-to-one binary
function.

22.   (New) A method according to Claim 20, wherein
each bit of the bit string is obtained by ANDing among the bits
of the 16-bit strings.

23.   (New) A device comprising:

a decoder for decoding an input byte and generating at
least one bit string that contains only one active bit;

an array of logic gates being input with the at least
one bit string, and generating a 256-bit string by logically
combining the bits of the at least one bit string according to
the one-to-one binary function; and

an encoder being input with the 256-bit string and
generating an output byte.

24.   (New) A device according to Claim 23, wherein
said decoder comprises a left decoder and a right decoder being
input with a left nibble and a right nibble of the input byte,
and generating a left 16-bit string and a right 16-bit string,
respectively, each containing only one active bit; said array of
logic gates generating the 256-bit string as a logic combination
of bits of the 16-bit strings.

25.   (New) A device according to Claim 24, wherein
said array of logic gates comprises an array of 256 AND gates,

each AND gate generating a respective bit of the 256-bit string by ANDing bits of the 16-bit strings.

26.   (New) A device according to Claim 24, further comprising:

an array of multiplexers each being input with bits of the 16-bit strings and being driven by selection signals, and generating a respective intermediate bit being fed to said array of logic gates; and

said array of logic gates generating bits of the 256-bit string by logically combining the intermediate bits.

27.   (New) A device according to Claim 23, wherein said decoder generates a corresponding auxiliary 256-bit string; and said array of logic gates generates the 256-bit string by changing an order of the bits of the auxiliary 256-bit string according to the one-to-one binary function.

28.   (New) A cryptographic device comprising:

a decoder for decoding an input byte and generating at least one bit string that contains at least one active bit;

an array of logic gates being input with the at least one bit string, and generating a 256-bit string by logically combining the bits of the at least one input string according to a one-to-one binary function; and

an encoder being input with the 256-bit string and generating an output byte.

29.   (New) A cryptographic device according to Claim 28, wherein the cryptographic device implements a Rijndael AES encryption/decryption algorithm.

30.   (New) A cryptographic device according to Claim 29, wherein the one-to-one function corresponds to a Bytesub operation within the Rijndael AES encryption/decryption algorithm.

31.   (New) A cryptographic device according to Claim 28, wherein said decoder comprises a left decoder and a right decoder being input with a left nibble and a right nibble of the input byte, and generating a left 16-bit string and a right 16-bit string, respectively, each containing only one active bit; said array of logic gates generating the 256-bit string as a logic combination of bits of the 16-bit strings.

32.   (New) A cryptographic device according to Claim 31, wherein said array of logic gates comprises an array of 256 AND gates, each AND gate generating a respective bit of the 256-bit string by ANDing bits of the 16-bit strings.

33.   (New) A cryptographic device according to Claim 31, further comprising:
an array of multiplexers each being input with bits of the 16-bit strings and being driven by selection signals, and generating a respective intermediate bit being fed to said array of logic gates; and
said array of logic gates generating bits of the 256-bit string by logically combining the intermediate bits.

34.   (New) A cryptographic device according to Claim 28, wherein said decoder generates a corresponding auxiliary 256-bit string; and said array of logic gates generates the 256-

6

bit string by changing an order of the bits of the auxiliary
256-bit string according to the one-to-one binary function.